AS-INTERFACE MASTER **NEWS**
Digital magazine by Bihl+Wiedemann
02/2024

Safety and security for (future-)safe automation

ASi-5 Safety and ASi Safety at Work – both with the option of also transmitting standard signals on the same line – plus a wide range of gateways and modules for implementing a variety of safety solutions regardless of industry or controller, as well as Safe Link for PLC-free, safe coupling and networking of ASi networks: the extensive portfolio underscores Bihl+Wiedemann's expertise in functional safety technology. But with digitalization in mechanical and plant engineering, safety is hardly conceivable without security – that is, without protection against cyberattacks. This is also the case for the automation specialists from Mannheim (Germany).

Functional safety serves to protect people and the environment from the risk of accidents that may originate from machines. Data and communication security is about monitoring operational technology (OT) structures and IT networks, as well as potential gateways, to reliably eliminate the risks posed by the manipulation or theft of data. As functional safety is becoming increasingly digitalized, safety solutions that do not take security risks into account can be exposed to the risk of external changes – changes that can impair or even negate their protective function.

ASi 5
SAFETY

When a replacement is needed, the hardware and safety configuration stored on the SD card, as well as the parameter data of the connected devices, can be completely transferred to a new gateway of the same type.

Security: new significance in legislation

It is not without reason that the EU Machinery Regulation 2023/1230, for example, which will replace the Machinery Directive 2006/42/EC on January 20, 2027, stipulates that machines must be designed and constructed in such a way that neither a connected device nor a remote device communicating with the machine can lead to a dangerous situation. This applies to hardware and software, both when the machine is used as intended and in the event of possible manipulation. Even the connection to or communication via remote access devices, such as routers, must not lead to dangerous situations.

The Cyber Resilience Act (CRA) of the European Union, which will harmonize the cybersecurity rules for products with digital elements throughout the EU and is also scheduled to apply from 2027, has the same thrust. And the latest revision of the Technical Rules for Operational Safety and Health (TRBS) of the German Federal Institute for Occupational Safety and Health also reflects the fundamental connection between safety and security. Safe automation therefore means considering and combining both aspects of the term “safety”.

Safety & security: two approaches to integration...

In principle, any device in a network with a connection to the IT world via TCP/IP can become a vehicle for attacks on other devices – and thus jeopardize production stability and process security.

One possible solution – as was common in the past and is still found to some extent today – would be to implement a safety solution without a link between the external fieldbus and IT world and the data network structure of a machine. Besides the fact that such decoupling no longer enables automated diagnostics of the safety technology, for example, it also goes against current and future trends in automation – i.e. digitalization and the implementation of Industry 4.0. And separate wiring of standard and safety components is no longer state of the art, not least because of the effort involved.

Assuming that innovative machine concepts in the sense of Industry 4.0 and business models based on them are unlikely without additional diagnostic and secondary data, including from the field of safety technology, the use of Ethernet-based safety technology in the field would be an alternative. Standardized and certified communication protocols such as PROFIsafe, FSoE or CIP Safety enable the transmission of safety related data in automation applications with functional safety.

However, each of these network components must have its own Ethernet connection and its own IP address, which must be individually secured regarding cybersecurity. This involves a great deal of work and high risk, especially when open Ethernet ports are freely accessible in the field. To make matters worse, the data collected for Industry 4.0 is often not transported via a separate IT interface, but also via the OT interface, for example, to a cloud. This means that there is no longer a barrier between the OT and IT worlds and the often-associated internet connections.

... and one simple solution: ASi-5 Safety

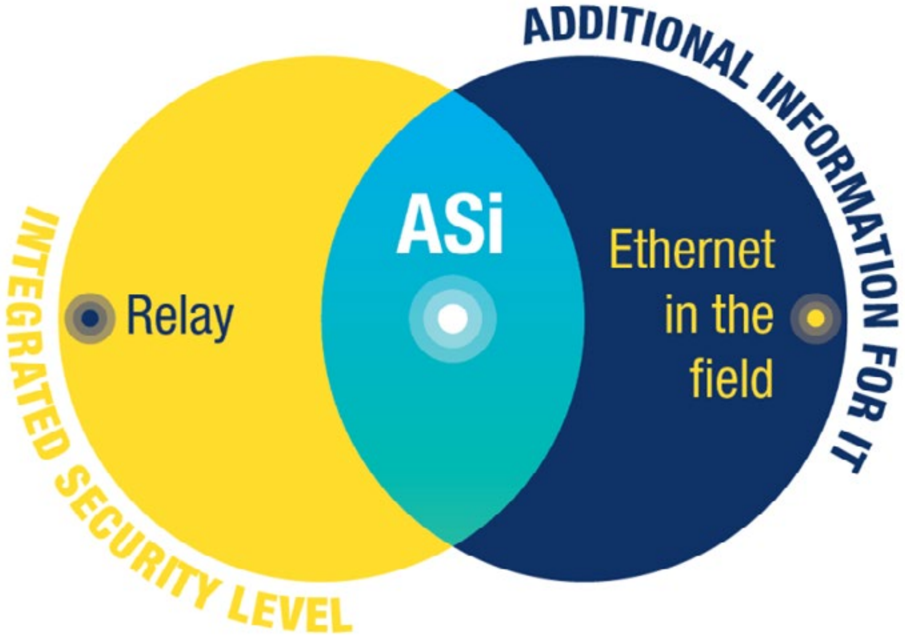
No connectors, one cable for standard and safety technology of different generations, best connection from any point in the network – AS-Interface, as the established wiring system for the lowest field level offers the possibility to realize machine safety more easily, cost-effectively, and customized than ever before. And arguably more efficiently than ever before. Because in contrast to a safe Ethernet-based communication, where each component requires its own IP address, ASi-5 Safety offers a much higher I/O density per IP address. Distributed over up to 2 x 200 m cable length, a gateway with ASi-5/ASi-3 safety monitor from Bihl+Wiedemann can easily manage well over 100 safe I/Os under one single IP address in two ASi networks and with I/O modules such as the new BWU4277 with 14 safe inputs and two electronic safe outputs. These, in turn, can be easily created and monitored in the company’s configuration software ASIMON360.

The safe signals, if necessary supplemented by standard signals, are collected exclusively via one single cable – the yellow ASi profile cable. This acts as the central nervous system in the OT network of a machine or installation and as a shuttle for safe signals to the ASi-5 Safety Gateway. The integrated safety monitor can be configured as a safety controller, thus making it possible to implement a safety application as a stand-alone solution.

However, since the gateways always have an integrated fieldbus interface such as PROFINET, EtherNet/IP, EtherCAT or POWERLINK, the higher-level control can be provided with extensive diagnostic information about the safety functions. When a gateway with a safe fieldbus protocol such as PROFISafe, CIP Safety or Safety over EtherCAT (FSoE) is used, not only the diagnostic data but also the secure data itself can be transmitted to a safe controller.

The gateway not only serves as a door opener to the world of intelligent ASi wiring technology with its broad portfolio of safety and standard I/O modules for the field, but also helps to reduce the number of Ethernet interfaces and thus significantly lowers the security risk within an installation. To make the additional data useful, all gateways with ASi-5 Safety also have a separate diagnostic interface that is optimized for the IT world.

This supports current IT communication standards such as OPC UA, REST API, and, in the future, MQTT. Thanks to the option of performing certificate-based, secure firmware updates in the field, new standards as well as new security requirements can be easily retrofitted and thus fulfilled – even in the field. To ensure high availability and minimal downtime in the event of a replacement, the hardware and safety configuration and the parameter data of the connected devices are stored on an SD card and transferred in full to a new, identical gateway when it is installed.



The communicative break between TCP/IP and field level in the gateway ensures that ASi can provide IT with a high level of available additional information, such as diagnostic data, while at the same time providing the best possible protection against cyberattacks.

ASi-5 Safety has security on board and in view

The high level of networking between Industry 4.0 devices and the risk that these will become a vehicle for attacks on other devices means that the security requirements for network nodes are increasing very rapidly. This is where the products from Bihl+Wiedemann deliver an impressive array of features and measures that ensure production stability and process reliability in the secure network.

Even if the ASi gateway with its connection to TCP/IP is the connection between the external fieldbus and IT world and the data network structure of a machine, it cannot become a point of entry or an attack platform for cyberattacks because it physically decouples the TCP/IP level and the field level with ASi and ASi Safety. This communicative break between ASi and TCP/ IP isolates the ASi network nodes from the outside, thereby preventing direct TCP/IP access to the field level in the first place.

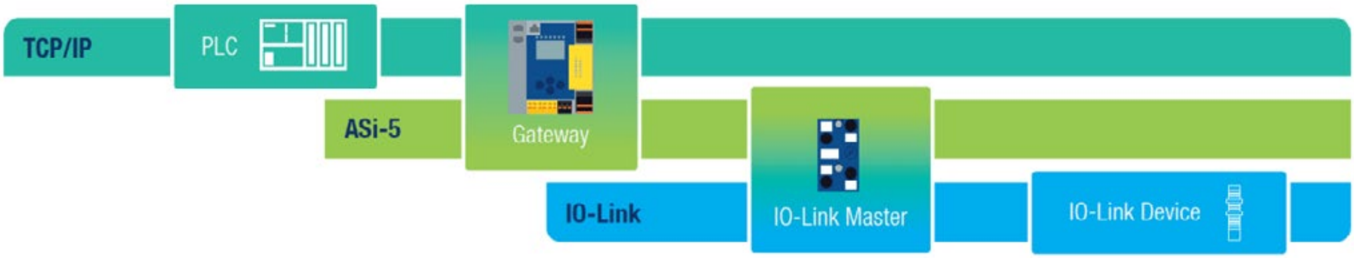
While the modules and nodes in the ASi network must meet far lower security requirements, as they cannot communicate in TCP/IP networks, the gateway is in principle the only component that is significantly relevant to cybersecurity. To protect ASi gateways, Bihl+Wiedemann carries out extensive tests with a wide range of cybersecurity tools during development and commissioning.

For example, the Ethernet fieldbus interface and the Ethernet diagnostic interface of the gateways are subjected to stringent resilience tests using the industry-proven Achilles® Robustness Test software from GE Digital to ensure that they are impervious to cyberattacks.

Security: comprehensive and future-proof

Due to the long service life of ASi products, it must also be possible to rectify detected vulnerabilities in the device software long after the devices have been placed in service. In addition, hackers and cybercriminals can pose new threats at any time, which are intended to circumvent existing security measures. True to the motto “The future on board and in view”, Bihl+Wiedemann therefore offers the option of updating safe parts of gateways during ongoing system operation by means of in-system firmware updates and signed security software to be authenticated by the device in advance as part of certificate-based end-to-end encryption. This enables the company’s ASi-5 modules to always be equipped with the latest security standards, making them investment-proof almost indefinitely.

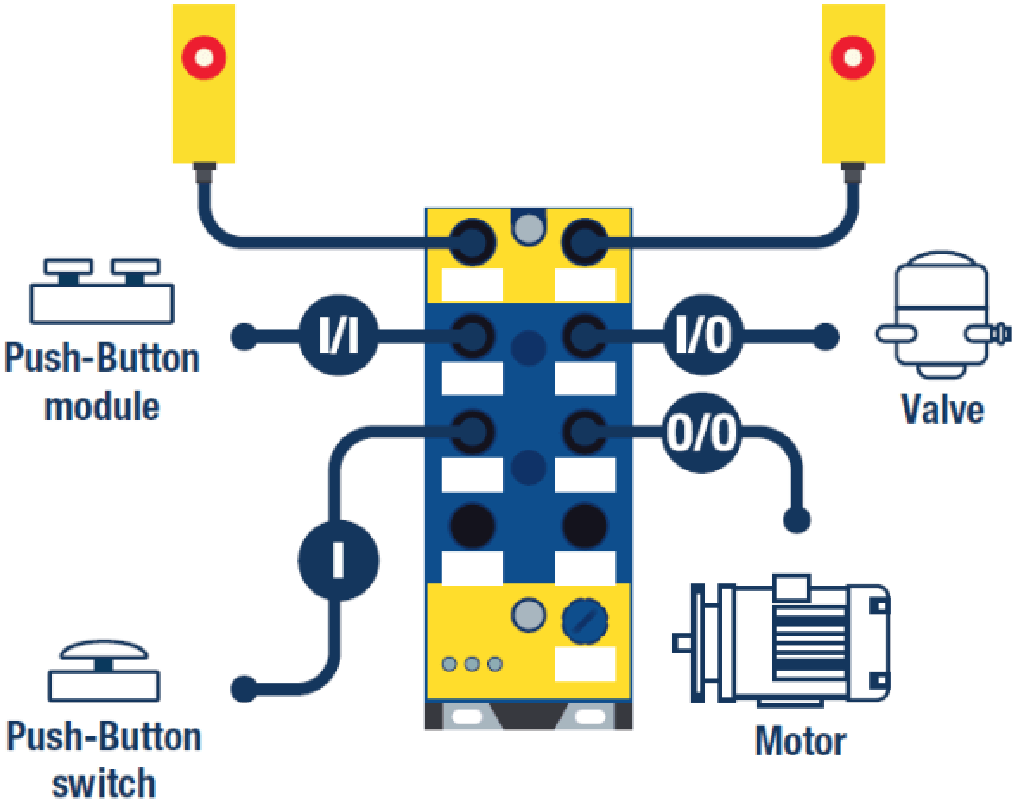
Other reasons why ASi-5 and ASi-5 Safety offer the highest level of cybersecurity include the use of cryptographic and authenticated encryption and verification algorithms such as AES-256 with SHA or RSA in Bihl+Wiedemann’s OPC-UA-capable products, as well as support for customer- specific certificates such as TLS. Secondly, ASi-5 uses Orthogonal Frequency- Division Multiplexing (OFDM) to transmit data. Due to this dynamic frequency allocation, recording the exchanged messages is very complex and only possible if the entire context of the connection setup, including the frequency changes between the ASi master and ASi node, is known.



The ASi-5/ASi-3 fieldbus gateway from Bihl+Wiedemann physically decouples TCP/IP from ASi-5 and ASi-5 Safety, i.e. the fieldbus and field level.

Safety & security: secure machines need both

The digital transformation in mechanical and plant engineering offers both the opportunity and the necessity to understand and implement machine safety and industrial cybersecurity as equally important aspects of safety technology. At Bihl+Wiedemann, this is consistently reflected in the company's products. As already seen in standard configurations with ASi-5, where its high performance has opened up numerous areas of application, using many new products since the introduction of the new standard – for example, in drive technology or in the integration of IO-Link devices – ASi-5 Safety also offers many new potentials for even smarter safety technology, taking into account all security aspects required in the future. This is because machine safety 4.0 can only be achieved through this kind of interaction between safety and security, ensuring not only functionality and cyberresilience but also financial security into the future.



Thanks to the combination of safe signals and standard signals in one module, ASi-5 Safety can cover almost all industry-relevant integration and application scenarios.